BLAISE PASCAL
Istituto di Istruzione Superiore Reggio Emilia
GRAFICA
INFORMATICA
RELAZIONI INTERNAZIONALI
SCIENZE APPLICATE

REGOLAMENTO
“SICUREZZA INFORMATICA”

LINEE GUIDA PER L'USO DELLE RISORSE TECNOLOGICHE E DI RETE

Scopi di una politica di uso sicuro delle risorse tecnologiche 2
Riferimenti normativi 3
Strategie della scuola per garantire la sicurezza informatica 4
Descrizione delle Risorse 5
Art. 1 - Postazioni informatiche e rete di Istituto: generalità 5
Art. 2 - Accesso alle postazioni informatiche 6
Art. 2.1 - Utilizzo delle postazioni da parte dei docenti 6
Art. 2.2 - Utilizzo delle postazioni informatiche da parte degli studenti 8
Art. 2.3 - Antivirus 11
Art. 2.4 - Dispositivi collegabili alla rete 11
Art. 3 - Account di Istituto per l'utilizzo di Google Workspace 11
Art. 4 - Sito Web dell'Istituto 12
Art. 5 - Registro Elettronico 13
Art. 6 - Servizio di Stampa 13
Art. 7 - Struttura del Sistema Informatico 14
Rete Cablata 14
Rete Wireless 14
Tracciamento e Monitoraggio 15
Manutenzione 15
Art. 8 - Accounting degli Utenti 15
Art. 9 - Tutela della privacy: garanzie generali 18
Art. 10 - Disposizioni di legge e sanzioni 19
Art. 11 - Norme conclusive 20

Scopi di una politica di uso sicuro delle risorse tecnologiche

Scopo del presente documento è quello di informare l'utenza al fine di garantire un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.
Lo sviluppo delle competenze digitali è uno degli obiettivi base del quadro europeo delle competenze chiave per l'apprendimento permanente. Naturalmente, rappresenta una delle principali competenze da acquisire nell'ambito del curricolo di Istituto del "Pascal".
Inoltre, il curricolo scolastico prevede che gli alunni imparino a cercare informazioni e materiale didattico, creare e condividere documenti e scambiare informazioni attraverso l'utilizzo delle tecnologie e degli strumenti digitali applicati alla didattica. La rete Internet offre sia agli alunni che ai docenti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi, risorse per il tempo libero, le attività scolastiche e sociali. Pertanto la Scuola promuove l'uso delle Tecnologie e degli Strumenti Digitali come supporto dei processi di insegnamento - apprendimento, nell'ottica di una didattica inclusiva, con opportunità e modalità diverse ai fini del successo formativo, cognitivo e psico-sociale degli alunni, per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.
Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti: è infatti dovere della Scuola garantire il diritto dei minori all'accesso alla rete e adottare nel contempo tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio nella navigazione.
Gli insegnanti hanno la responsabilità di guidare gli alunni nelle attività on-line, di stabilire obiettivi chiari nell'uso di Internet e insegnarne un uso accettabile e responsabile, di individuare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa al fine di prevenire il verificarsi di situazioni potenzialmente pericolose.
Il personale di segreteria, nella gestione degli aspetti amministrativi dell'Istituto fa largo uso delle tecnologie informatiche, nell'ottica della dematerializzazione degli atti oltre che per una efficiente ed efficace comunicazione.
Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti, o al reperimento ed uso di materiali inappropriati.
La scuola ha elaborato questo documento in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e

cyberbullismo (aprile 2015) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione. Si segnala la pubblicazione della nota del 23 marzo 2021, n. 774 relativa all'implementazione del percorso di formazione per docenti e Dirigenti scolastici su Piattaforma ELISA, sul sito dell'Ufficio Scolastico Regionale per l'Emilia-Romagna (al link diretto: https://www.istruzioneer.gov.it/2021/03/26/formazione-e-learning-piattaforma-elisa-prevenzione-bullismo-e-cyberbullismo).
Sempre sul sito web www.istruzioneer.gov.it sono disponibili le Linee Guida di Orientamento, Prevenzione e Contrasto del bullismo e del cyberbullismo, aggiornate nel 2021 (al link:
https://www.istruzioneer.gov.it/2021/03/05/linee-di-orientamento-prevenzione-e-contrasto-bullismo-e-cyberbullismo-2021/).
Le regole approvate nel presente disciplinare tecnico devono avere una valenza formativa e non solo sanzionatoria, perché il loro scopo è quello di aiutare gli utenti meno esperti a orientarsi in merito a temi quali la privacy, la libertà di espressione, il plagio, l'identificazione ed identità di rete, l'etica nella rete, i vincoli legali, le molestie, l'utilizzo delle risorse.
Le linee guida si propongono di perseguire le seguenti finalità:

- garantire la massima efficienza delle risorse;
- garantire la riservatezza delle informazioni e dei dati;
- provvedere ad un servizio continuativo nell'interesse della comunità scolastica;
- provvedere ad un'efficiente attività di monitoraggio;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche;
- garantire la massima sicurezza nell'interazione tra l'Istituto e gli altri soggetti pubblici o privati e ottimizzare i costi di esercizio;
- garantire il rispetto delle leggi in materia di protezione dei dati.

Riferimenti normativi

II presente documento è stato redatto in conformità alle seguenti disposizioni normative, per quanto attiene al settore scolastico:

- L. 547/ 1993: norme in materia di reati informatici;
- D.P.R. n. 275 del 25/02/1999, Regolamento recante norme in materia di autonomia delle istituzioni scolastiche, ai sensi dell'alt. 21 della legge 15 marzo 1997, n. 5;
- L. 325/2000 sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'alt. 15 della L. 675/1996;
- C. M. 114/2002, Sulle infrastrutture tecnologiche nelle scuole e nuove modalità di accesso al sistema informativo;
- D.lgs 196/2003 T.U. sulla privacy entrato in vigore il 1/1/2004 che riassume le norme precedenti sulla privacy;
- L. 4/2004, Disposizioni per favorire l'accesso dei soggetti disabili agli

strumenti informatici;
- Raccomandazione del Parlamento Europeo e del Consiglio del 18/12/2006 (competenza digitale come competenza chiave);
- L. 107/2015, che tra gli obiettivi educativi prioritari pone lo sviluppo delle competenze digitali e l'adozione del Piano Nazionale della Scuola Digitale;
- Codice comportamentale MIUR 28/11/2016;
- Regolamento UE 2016/679, Regolamento generale sulla protezione dei dati personali;
- L. 71/2017, Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo;
- Nota 482 del 18 febbraio 2021, Linee di Orientamento per la prevenzione e il contrasto del Bullismo e del Cyberbullismo;
- L. 92/2019, Introduzione all'insegnamento dell'educazione civica.

Strategie della scuola per garantire la sicurezza informatica

Al fine di garantire una gestione il più possibile corretta delle dotazioni tecnologiche, l'Istituto attua le seguenti strategie:
- il sistema informatico dell'Istituto viene regolarmente controllato in base alle norme di sicurezza;
- è predisposta una separazione logica tra la rete didattica e quella amministrativa;
- il sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente;
- la connessione WiFi ad Internet dell'Istituto è regolata da un meccanismo di autenticazione-autorizzazione e da tecniche di filtraggio;
- l'uso dei dispositivi presenti e l'utilizzo dei laboratori didattici è regolamentato come descritto nell'allegato "Regolamento di gestione e utilizzo dei Laboratori Didattici e delle Strumentazioni Tecnologiche";
- i software installati sono autentici e aggiornati.

Sono attivate strategie di informazione sull'uso consapevole della rete:
- avvio di percorsi di formazione ad un uso consapevole delle tecnologie digitali rivolti ai docenti;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti (si fa riferimento al "Patto Educativo di Corresponsabilità" di Istituto);
- costante e aggiornata informazione agli utenti sui pericoli della rete in relazione all'evoluzione delle tecnologie in collegamento con le Forze di Polizia e gli Enti preposti;
- controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, temp, cookies, ecc.) da parte dei responsabili dell'attività informatica;

- utilizzo di firewall e proxy;
- settaggio delle macchine in modo che agli utenti non sia consentito di scaricare e/o installare alcun tipo di software.

Descrizione delle Risorse

Al fine del corretto utilizzo nonché nell'ottica di una gestione efficiente ed efficace di tutto l'Istituto si rende necessario individuare tutte le risorse tecnologiche informatiche di cui l'Istituto dispone e regolamentare il loro utilizzo.

L'Istituto dispone di tecnologie informatiche sia per lo svolgimento delle attività didattiche e laboratoriali che per il funzionamento amministrativo:

- laboratori informatici provvisti di una postazione per ogni studente (con accesso cablato alla rete Intranet e Internet);
- aule attrezzate provviste di postazione per il docente (con accesso cablato alla rete Intranet e Internet) e sistema di videoproiezione e/o digital board;
- kit di proiezione portatili, comprensivi di PC e videoproiettore (con accesso wireless alla rete Internet);
- laboratori mobili (con accesso wireless alla rete Internet);
- aule riservate ai docenti, provviste di postazioni fisse (con accesso cablato alla rete Intranet e Internet) e di spazi per l'utilizzo di device personali (con connessione cablata e/o wireless alla rete Internet);
- uffici con postazioni fisse per il personale amministrativo e tecnico (con accesso cablato alla rete Intranet e Internet);
- postazioni per il personale ausiliario (con accesso cablato alla rete Internet);
- stampanti di rete (disponibili previo accounting);
- notebook (con accesso wireless alla rete Internet) a disposizione di docenti e studenti per l'utilizzo legato ad attività temporanee e di breve durata.

L'Istituto dispone di due reti logicamente separate, utili per l'accesso a Internet ed Intranet, rispettivamente per l'aspetto amministrativo e didattico.

Art. 1 - Postazioni informatiche e rete di Istituto: generalità

L'accesso alle postazioni fisse e alla rete Intranet da parte del personale e degli studenti è vincolata da un sistema di accounting personale.

Anche l'accesso alla rete wireless da parte del personale docente e ATA è protetta da misure di sicurezza legate ad un sistema di accounting personale (gestito da Federa - Lepida S.p.A.).

Gli alunni non possono accedere alla rete wireless, se non limitatamente

all'effettuazione di attività specifiche (dietro richiesta del docente di riferimento) e comunque legate ad un sistema di accounting personale (gestito da Federa - Lepida S.p.A.). da modificare?

E' fatto divieto di utilizzare la rete dell'Istituto per finalità non previste dal presente regolamento o non espressamente autorizzate.

La navigazione è consentita nel rispetto delle seguenti condizioni:

a. utilizzo della rete per i soli scopi legati alle attività didattico-amministrative;
b. rispetto della netiquette (si veda l'allegato "Netiquette - etica e norme di buon uso dei servizi di rete");
c. divieto di monitoraggio di ciò che transita in rete se non nelle forme e nei limiti previsti nel presente regolamento.

Per problemi correlati alla sicurezza della rete locale, l'Istituto dispone di un sistema di controllo (firewall) che registra tutte le attività sulla rete; il fine è quello di individuare, in caso di necessità, eventuali utilizzi fraudolenti della rete di Istituto, della quale è direttamente responsabile il Dirigente Scolastico; infatti, come definito anche dalle linee guida del Garante, il datore di lavoro (il DS), secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104, può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro; tuttavia, ciò deve essere fatto nel rispetto delle norme poste a tutela del lavoratore (ci si riferisce, in particolare, al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" di cui all'art. 4 della legge 300 del 1970). Pertanto il datore di lavoro potrebbe, ad esempio, verificare se vi è stato indebito utilizzo della connessione ad Internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione, senza però indagare sul contenuto dei siti visitati.

Art. 2 - Accesso alle postazioni informatiche

Tutti i docenti hanno il diritto di poter accedere alle postazioni singolarmente, per le attività connesse alla funzione docente, e con gli studenti per le attività didattiche.

L'utilizzo delle postazioni nelle aule riservate ai docenti è ad accesso libero, previo accounting. I docenti che non hanno dei laboratori di riferimento possono richiedere, previa prenotazione, l'uso dei laboratori mobili o dei kit di proiezione o dei singoli notebook. La prenotazione dei laboratori mobili, dei kit di proiezione e degli altri dispositivi avviene tramite l'utilizzo di portale riservato (accessibile tramite login solo dal personale dell'Istituto).

Art. 2.1 - Utilizzo delle postazioni da parte dei docenti

I docenti che utilizzano le postazioni informatiche (nelle aule insegnanti o

nelle aule didattiche o nei laboratori o i kit di videoproiezione) sono tenuti a:

a. assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da loro stessi utilizzata, segnalando prontamente eventuali malfunzionamenti agli assistenti tecnici (tramite l'utilizzo di modulo predisposto o tramite chiamata diretta);
b. segnalare prontamente eventuali danneggiamenti o mancanze all'ufficio tecnico;
c. non divulgare le credenziali di accesso (ai dispositivi fissi, alla rete WiFi, alle caselle di posta istituzionali, al captive portal per l'accesso a Internet, al sistema di prenotazione aule, al registro elettronico, a piattaforme didattiche);
d. dopo aver effettuato l'accesso al proprio account, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, senza aver effettuato la disconnessione;
e. non salvare sulla memoria locale dei dispositivi dell'Istituto file, soprattutto se contengono dati personali e/o sensibili;
f. collegare dispositivi di memorizzazione portatili personali solo previa scansione con software antivirus apposito;
g. utilizzare le strumentazioni (PC, stampanti, webcam) e l'accesso alla rete Intranet ed Internet dell'Istituto per le sole finalità connesse alla funzione docente;
h. utilizzare le sole caselle di posta elettronica istituzionali (@iispascal.it e @posta.istruzione.it);
i. conoscere le regole base di protezione dai rischi derivanti dall'utilizzo della rete (phishing, spam, ...);
j. non scaricare materiale digitale per fini personali e/o protetto da copyright;
k. evitare di visitare siti non necessari ad una normale attività didattica.

I docenti che utilizzano i laboratori (anche mobili) hanno l'obbligo di vigilare sul corretto utilizzo delle stesse da parte degli studenti sia quando operano singolarmente che in gruppo.

In particolar modo ogni docente è tenuto:

a. ad illustrare ai propri allievi le regole di utilizzo contenute nel presente documento (si sottolinea che tutti gli studenti seguono unità formative specifiche sulla sicurezza dei laboratori);
b. a controllare che l'accesso degli alunni alla rete Internet e Intranet avvenga sempre e nel rispetto del presente Regolamento;
c. a dare chiare indicazioni sul corretto utilizzo della rete (Intranet, Internet, piattaforme online,...), condividendo con gli alunni la netiquette e vigilando sul rispetto della stessa;
d. ad assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da lui

stesso e dagli alunni utilizzata, segnalando prontamente eventuali malfunzionamenti agli assistenti tecnici (tramite l'utilizzo di modulo predisposto o tramite chiamata diretta);

e. a sollecitare gli alunni a segnalare prontamente eventuali danneggiamenti o mancanze e riportarle all'ufficio tecnico;
f. a sollecitare gli alunni a non divulgare le credenziali di accesso (ai dispositivi fissi, alla casella di posta istituzionale, al captive portal per l'accesso a Internet, al registro elettronico, a piattaforme didattiche);
g. a sollecitare gli alunni a, dopo aver effettuato l'accesso al proprio account, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, senza aver effettuato la disconnessione;
h. a sollecitare gli alunni a non salvare sulla memoria locale dei dispositivi dell'Istituto file contenenti dati personali e/o sensibili;
i. a sollecitare gli alunni a collegare dispositivi di memorizzazione portatili solo previa scansione con software apposito;
j. a sollecitare gli alunni a utilizzare gli strumenti (PC, stampanti, webcam) e l'accesso alla rete Intranet ed Internet dell'Istituto per le sole finalità connesse alla attività didattica;
k. a sollecitare gli alunni a utilizzare le sole caselle di posta elettronica istituzionali (@studenti.iispascal.it);
l. ricordare agli alunni le regole base di protezione dai rischi derivanti dall'utilizzo della rete (phishing, spam, ...);
m. proporre agli alunni attività di ricerca di informazioni in rete principalmente fornendo loro, almeno inizialmente quale opportuno riferimento guida, indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento (creati per la didattica, istituzionali e/o preventivamente verificati dall'insegnante stesso).

E' compito del personale Ausiliario custodire le chiavi, aprire e chiudere i laboratori.
Copia delle chiavi di ogni laboratorio viene custodito anche nell'ufficio degli assistenti tecnici.

Art. 2.2 - Utilizzo delle postazioni informatiche da parte degli studenti

Gli studenti possono utilizzare tutti i dispositivi elettronici (PC dei laboratori e della biblioteca, notebook portatili, notebook tablet dei laboratori mobili) di cui l'Istituto dispone, sotto la guida e vigilanza dei docenti referenti ed in conformità con il progetto educativo, nel rispetto del seguente regolamento e dell'allegato "Regolamento di gestione e utilizzo dei Laboratori Didattici e delle Strumentazioni Tecnologiche". Ogni studente dispone di un account per l'accesso alla Intranet di Istituto e di un account per l'accesso alla rete wireless (tramite captive portal gestito da Federa - Lepida S.p.A.).
Per gli studenti, è disponibile l'accesso alla piattaforma Google Workspace

for Education, attraverso l'attivazione di un account personale con password. Attraverso la piattaforma è possibile scaricare e caricare compiti, materiali didattici, lezioni e comunicare con i docenti della propria classe. (si veda l'allegato "Regolamento di gestione e utilizzo di Google Workspace").

Gli studenti hanno accesso al Registro Elettronico, attraverso l'attivazione di un account personale con password. Attraverso il registro elettronico è possibile visualizzare comunicazioni, compiti, note, voti, assenze. (si veda l'allegato "Regolamento di gestione e utilizzo del Registro Elettronico").

Gli studenti possono interagire anche con il sito ufficiale della scuola dal quale è possibile visualizzare varie sezioni tra cui l'Albo d'Istituto e le comunicazioni relative all'anno scolastico in corso, cui può accedere qualunque utente della rete compresi i genitori.

L'utilizzo da parte degli studenti dei dispositivi digitali sia nei lavori di gruppo che nelle attività individuali avviene nel rispetto delle seguenti regole:

a. utilizzare i dispositivi nonché l'accesso in rete, sempre sotto la supervisione del docente;
b. accedere all'ambiente di lavoro con il proprio account personale;
c. assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da loro stessi utilizzata, segnalando prontamente eventuali malfunzionamenti, danneggiamenti o mancanze al docente di riferimento
d. non divulgare le credenziali di accesso (ai dispositivi fissi, alla casella di posta istituzionale, al captive portal per l'accesso a Internet, al registro elettronico, a piattaforme didattiche);
e. dopo aver effettuato l'accesso al proprio account, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, senza aver effettuato la disconnessione;
f. archiviare i propri documenti in maniera ordinata nella propria cartella di rete e non nella memoria locale del dispositivo;
g. non eseguire tentativi di modifica della configurazione di sistema delle macchine;
h. non eseguire tentativi di monitoraggio dei dati presenti nella rete:
i. accedere alla rete solo in presenza o con l'autorizzazione dell'insegnante responsabile dell'attività;
j. non utilizzare i dispositivi e l'accesso a Internet della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
k. chiudere correttamente la propria sessione di lavoro;
l. collegare dispositivi di memorizzazione portatili solo previa scansione con software antivirus apposito;

m. utilizzare la sola casella di posta elettronica istituzionale (@studenti.iispascal.it);
n. conoscere le regole base di protezione dai rischi derivanti dall'utilizzo della rete (phishing, spam, ...);
o. non scaricare materiale digitale per fini personali e/o protetto da copyright;
p. non visitare siti non necessari ad una normale attività didattica.

In particolare modo gli studenti, al fine di favorire l'integrazione e l'accesso alle tecnologie informatiche anche ai compagni meno preparati, sono tenuti al rispetto delle seguenti buone prassi (lotta al cyberbullismo):

a. rispettare le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi;
b. non essere intolleranti con chi ha scarsa dimestichezza con le tecnologie informatiche o commette errori concettuali;
c. non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
d. richiedere sempre il permesso ai genitori, in caso di minori, prima di iscriversi a qualche mailing-list o sito web che lo richieda;
e. non dare indirizzo e numero di telefono a persone incontrate sul web, in caso di minori, senza chiedere il permesso ai genitori (questo perché non si può avere la certezza dell'identità della persona con la quale si sta comunicando);
f. non prendere appuntamenti con le persone conosciute tramite web, in caso di minori, senza aver interpellato prima i genitori;
g. non inviare foto, filmati, o altro materiale riconducibile alla propria persona senza aver chiesto, in caso di minori, preventivamente il consenso dei propri genitori;
h. non inviare foto, filmati, o altro materiale riconducibile ad altre persone senza avere prima richiesto il consenso del diretto interessato, ovvero nel caso di minori il consenso dei rispettivi genitori;
i. riferire sempre a insegnanti e genitori se si è raggiunti in rete da immagini o scritti che infastidiscono;
j. se qualche studente dovesse venire a conoscenza che altri compagni non rispettano le suddette regole è opportuno parlarne con gli insegnanti e con i genitori;
k. chiedere il permesso ai genitori, nell'ipotesi di minori che utilizzano postazioni internet nelle proprie abitazioni, ovvero agli insegnanti, nell'ipotesi di apparecchiature scolastiche, prima di scaricare dal web materiale di vario tipo;
l. seguire le regole della Netiquette (si veda l'allegato "Netiquette - Etica e Norme di buon uso dei servizi di rete").

Art. 2.3 - Antivirus

II personale che accede alle postazioni informatiche della scuola deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della scuola mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc). A tal fine il personale è tenuto:

a. verificare mediante il software antivirus presente nei dispositivi ogni dispositivo di provenienza esterna alla scuola prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, il dispositivo non dovrà essere utilizzato;
b. nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto agli assistenti tecnici informatici.

Art. 2.4 - Dispositivi collegabili alla rete

Per attività connesse all'attività didattica/amministrativa, possono essere connessi alla rete cablata e alla rete wireless dispositivi anche di natura privata.

Per quanto riguarda la rete cablata, al momento dell'accesso ad Internet viene richiesto l'accounting da captive portal attraverso le credenziali di dominio, per il tracciamento del traffico.

Per quanto riguarda la rete wireless, a seguito dell'accesso alla rete, per poter effettuare la navigazione occorre autenticarsi presso il gestore della rete (Federa - Lepida S.p.A.), che provvede anche al tracciamento del traffico Internet.

In tale ipotesi, il personale che vorrà avvalersi di propri dispositivi collegabili alla rete dovrà rispettare le norme previste nell'allegato "Regolamento BYOD".

Art. 3 - Account di Istituto per l'utilizzo di Google Workspace

L'account istituzionale (nome.cognome@iispascal.it per il personale, nome.cognome@studenti.iispascal.it per gli studenti), è uno strumento legato alla finalità didattico-amministrative e alle attività ad esso connesse. Il personale della scuola titolare di casella di account di Istituto è responsabile del corretto utilizzo della stessa (art.615-quater c.p.).

L'utilizzo dello stesso, in particolar modo della casella di posta elettronica, deve avvenire nel rispetto delle seguenti buone prassi

a. utilizzare l'account solo per scopi professionali;
b. non aprire messaggi di posta elettronica insoliti o provenienti da sconosciuti, per non correre il rischio di essere infettati da virus (occorrerà cancellare i messaggi senza aprirli). Anche i messaggi provenienti da conosciuti possono contenere file eseguibili (quindi virus), pertanto bisogna fare attenzione alle estensioni dei file allegati (anche questi ultimi non devono essere aperti);
c. bloccare messaggi che diffondono "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata);
d. per l'invio di file ad altre istituzioni pubbliche o private è preferibile utilizzare un formato protetto da scrittura;
e. utilizzare l'account per l'iscrizione a mailing list o piattaforme solo per uso professionale
f. cancellare dall'account i documenti ritenuti inutili al fine di evitare l'occupazione di spazio di memoria.

Si fa riferimento all'allegato "Regolamento di gestione e utilizzo di Google Workspace".

Art. 4 - Sito Web dell'Istituto

La responsabilità e la gestione del sito web dell'Istituto è del rappresentante legale, ovvero del Dirigente Scolastico. La gestione del sito è affidata dal Dirigente Scolastico ad un docente, indicato come "referente del sito web di Istituto".
Il sito web (www.pascal.edu.it) si pone come strumento informativo interno ed esterno, di comunicazione di contenuti educativi e di attività didattico-formative. L'istituto detiene i diritti d'autore dei documenti prodotti in proprio o dei quali è stato chiesto e ottenuto il permesso di pubblicazione. Nella pubblicazione di immagini degli alunni minorenni è necessaria la preventiva liberatoria da parte dei genitori. Anche in presenza di liberatoria, l'Istituto procede con la massima attenzione, preferendo pubblicare immagini a campo lungo, senza primi piani; immagini di gruppo in attività piuttosto che di singoli. Il sito rispetta, in parte, i requisiti di accessibilità per i disabili di cui alla L.9/1/2004 (si veda dichiarazione di accessibilità reperibile al link…)
Nel sito dell'Istituto sono presenti tutte le informazioni relative all'organizzazione della scuola: P.T.O.F., Regolamenti, contatti, ...

Dal sito è possibile anche collegarsi al registro elettronico, all'area riservata per la prenotazione di aule e laboratori, a siti istituzionali.

Si fa riferimento all'allegato "Regolamento di gestione del sito del Sito Web istituzionale".

Art. 5 - Registro Elettronico

I docenti che interagiscono con il registro elettronico (ClasseViva - gruppo Spaggiari) oltre a quanto previsto nel presente documento, in materia di fruizione di tecnologie informatiche, devono rispettare le seguenti prescrizioni:

a. aggiornare tempestivamente il registro elettronico in tempo reale relativamente alle presenze degli alunni in classe, alle annotazione dei ritardi e delle assenze;
b. aggiornare tempestivamente, le valutazioni, gli argomenti delle lezioni ed altre eventuali annotazioni;
c. cambiare periodicamente le password, rispettando la dimensione e la tipologia dei caratteri suggerite dalla piattaforma;
d. non lasciare incustoditi dispositivi in cui è attivo il collegamento alla piattaforma;
e. non comunicare la password di accesso ed evitare che le stesse siano presenti su supporti cartacei o digitali;
f. non memorizzare nel browser di dispositivi (personali e non) la password di accesso.

Si fa riferimento all'allegato "Regolamento di gestione e utilizzo del Registro Elettronico".

Art. 6 - Servizio di Stampa

Il servizio di stampe e fotocopie è gestito attraverso stampanti professionali collegate alla rete cablata dell'Istituto (sia nella sede centrale che nelle sedi distaccate).
I docenti e il personale che necessiti di stampe o fotocopie può utilizzare le stampanti di rete da qualunque PC collegato alla rete cablata.
Per motivi legati alla sicurezza e alla privacy, oltre che per il tracciamento dell'utilizzo delle risorse, ogni utente del servizio di stampa possiede un PIN personale che deve digitare per attivare il fotocopiatore.
Anche i fotocopiatori seguono la suddivisione fra rete didattica e amministrativa.
Nell'utilizzo del servizio di stampa occorre rispettare le seguenti prescrizioni:

a. effettuare stampe e/o fotocopie esclusivamente per fini didattico-amministrativi;
b. non comunicare il proprio PIN;
c. cercare di evitare sprechi di risorse: carta e toner (stampe fronte/retro, solo stampe indispensabili,...).

Art. 7 - Struttura del Sistema Informatico

Rete Cablata

Il sistema informativo dell'Istituto è composto da due reti (didattica e amministrativa) logicamente separate, che condividono solamente l'accesso esterno alla rete Internet.
La gestione degli account degli utenti avviene tramite Active Directory ed è gestita dall'amministratore di Sistema (personale tecnico informatico).
L'account permette l'accesso ai PC fissi presente nell'Istituto (per docenti e studenti nell'area didattica, per il personale nell'area amministrativa).
Per quanto riguarda la rete didattica:

- ogni docente dispone di una propria cartella di rete, su cui ha diritti di lettura e scrittura;
- ogni studente dispone di una propria cartella di rete, su cui ha diritti di lettura e scrittura;
- ogni classe dispone di una cartella condivisa, nella quale i docenti hanno diritto di lettura e scrittura, mentre gli studenti hanno diritto di sola lettura (nella quale è fatto divieto di inserire documenti che contengono dati sensibili);
- ~~esiste una cartella condivisa fra tutto il personale docente, per lo scambio di documenti e materiali (nella quale è fatto divieto di inserire documenti che contengono dati sensibili);~~
- i docenti di informatica hanno diritto di accesso alle cartelle degli studenti, per attività di controllo e di raccolta delle prove di laboratorio;
- esiste una cartella accessibile in scrittura dai docenti di informatica e in lettura dagli studenti, per lo scambio di materiale di grandi dimensioni.

Per quanto riguarda la rete amministrativa:

- ogni utente degli uffici dispone e di una propria cartella di rete, su cui ha diritti di lettura e scrittura;
- esiste una cartella condivisa fra il personale del medesimo ufficio (didattica, personale, amministrativo) per lo scambio di documenti;
- il DSGA ha accesso a tutte le cartelle condivise.

Rete Wireless

Tutte le sedi dell'Istituto sono coperte da segnale Wireless. Le reti in essere sono:

- Pascal-WiFi: rete utilizzabile dai soli docenti per l'accesso a Internet dei dispositivi mobili (per poter effettuare la navigazione si accede attraverso password security mode WPA2 e occorre autenticarsi presso il gestore della rete Federa - Lepida S.p.A.);
- Pascal-Registro: rete utilizzabile dai soli docenti che permette l'accesso solamente al portale del Registro Elettronico e al sito della scuola (si accede attraverso password security mode WPA2);
- Pascal-Studenti: rete utilizzabile dagli studenti, attivata solo in caso di effettiva necessità e dietro richiesta di un docente (per poter effettuare la navigazione si accede attraverso password security mode WPA2 e occorre autenticarsi presso il gestore della rete Federa - Lepida S.p.A.);

- Pascal-Ospiti: rete attivabile in caso di eventi che richiedano l'utilizzo della rete Internet anche a personale esterno alla scuola (per poter effettuare la navigazione si accede attraverso password security mode WPA2 e non occorre autenticarsi presso il gestore della rete Federa - Lepida S.p.A., ma occorre autenticarsi con account di dominio Intranet)

Tracciamento e Monitoraggio

Per quanto riguarda la rete cablata, il tracciamento della navigazione avviene attraverso un sistema di firewall, con il quale avviene anche il filtraggio sulle richieste di siti potenzialmente dannosi, social network, piattaforme di gaming e il controllo di eventuali virus.
Per quanto riguarda la rete wireless, il tracciamento della navigazione viene effettuato dal gestore della rete (Federa - Lepida S.p.A.).
Il monitoraggio della rete wireless avviene in tempo reale attraverso il controller wifi di rete che quantifica dispositivi collegati in quel momento.
Il monitoraggio dei dispositivi di rete cablati avviene attraverso il sistema Observium che controlla sia il traffico di rete che la funzionalità degli stessi.

Manutenzione

Tutti i dispositivi dell'istituto vengono controllati costantemente sia in termini di funzionalità che di sicurezza.
I PC dei laboratori vengono ripristinati (attraverso immagine di sistema) all'inizio di ogni anno scolastico e ogni volta che necessitano un reset completo del sistema.
I dispositivi mobili, i kit di videoproiezione vengono controllati periodicamente, ad intervalli regolari, dagli assistenti tecnici informatici

Art. 8 - Accounting degli Utenti

Personale, studenti e genitori sono proprietari di differenti account relativi al sistema informativo di Istituto.

Docenti:
- Intranet: l'account permette l'accesso ai dispositivi fissi appartenenti alla rete didattica;
- Google Workspace: account per l'accesso ai servizi della Google Workspace (iispascal.it);
- Registro Elettronico: account per l'accesso al registro elettronico (ClasseViva - gruppo Spaggiari);
- Prenota: account per l'accesso al servizio di prenotazione di aule e dispositivi, gestito da un docente di riferimento (accessibile attraverso link presente sul sito istituzionale)
- Federa: accesso al captive portal del gestore della rete wireless (Federa - Lepida S.p.A.) tramite SPID;
- servizio di stampa: PIN per l'utilizzo dei fotocopiatori;

- portali ministeriali: alcuni docenti hanno accesso a portali ministeriali particolari, a seguito di funzioni ricoperte nel middle-managment di Istituto

Personale Amministrativo:
- Intranet: l'account permette l'accesso ai dispositivi fissi appartenenti alla rete amministrativa;
- Google Workspace: account per l'accesso ai servizi della Google Workspace (iispascal.it);
- Registro Elettronico: account per l'accesso al registro elettronico (ClasseViva - gruppo Spaggiari)
- Federa: accesso al captive portal del gestore della rete wireless (Federa - Lepida S.p.A.) tramite SPID;
- servizio di stampa: PIN per l'utilizzo dei fotocopiatori;
- portali ministeriali: alcuni assistenti amministrativi hanno accesso a portali ministeriali particolari, a seguito di funzioni facenti parte dell'incarico ricoperto.

Personale Tecnico:
- Intranet: l'account permette l'accesso ai dispositivi fissi appartenenti a tutta la rete;
- Google Workspace: account per l'accesso ai servizi della Google Workspace (iispascal.it);
- Registro Elettronico: account per l'accesso al registro elettronico (ClasseViva - gruppo Spaggiari)
- Federa: accesso al captive portal del gestore della rete wireless (Federa - Lepida S.p.A.) tramite SPID;
- servizio di stampa: PIN per l'utilizzo dei fotocopiatori.
- servizi di dominio: alcuni assistenti tecnici hanno accesso alla gestione dei servizi delle reti Intranet e Internet, a seguito di funzioni facenti parte dell'incarico ricoperto.

Personale Ausiliario:
- Intranet: l'account permette l'accesso ai dispositivi fissi appartenenti alla sola rete didattica;
- Google Workspace: account per l'accesso ai servizi della Google Workspace (iispascal.it);
- Registro Elettronico: account per l'accesso al registro elettronico (ClasseViva - gruppo Spaggiari)
- Federa: accesso al captive portal del gestore della rete wireless (Federa - Lepida S.p.A.) tramite SPID;
- servizio di stampa: PIN per l'utilizzo dei fotocopiatori.

Studenti:
- Intranet: l'account permette l'accesso ai dispositivi fissi appartenenti alla rete didattica;

- Google Workspace: account per l'accesso ai servizi della Google Workspace (iispascal.it);
- Registro Elettronico: account per l'accesso al registro elettronico (ClasseViva - gruppo Spaggiari);
- Federa: account per l'accesso al captive portal del gestore della rete wireless (Federa - Lepida S.p.A.), per gli studenti maggiorenni questo può essere sostituito da accesso tramite SPID;

Genitori:
- Registro Elettronico: account per l'accesso al registro elettronico (ClasseViva - gruppo Spaggiari);
- Google Workspace del figlio, se minore: account per l'accesso ai servizi della Google Workspace (iispascal.it);

Le password degli account devono essere predisposte nel rispetto delle seguenti tecniche di sicurezza:
- utilizzare il numero dei caratteri previsti dal sistema;
- non deve contenere la username come sua parte;
- non deve essere simile alla precedente;
- deve contenere caratteri numerici e alfabetici;
- non utilizzare caratteri e dati facilmente riconducibili al titolare della password (es. nome/cognome, data di nascita, hobby, nome ci persone care, ecc);
- non usare acronimi comuni come parte della password.
- non usare parole comuni o invertire l'ortografia delle parole come parte della password.
- non utilizzare nomi di persone o luoghi, come parte della password.
- modificare frequentemente le password.

Norme per la Protezione della Password
- Non annotare mai la password, ma memorizzare la password evitando supporti cartacei o digitali come promemoria;
- Non inviare mai una password tramite e-mail.
- Non includere una password documento archiviato non-crittografato.
- Non rivelare mai a nessuno le proprie password.
- Non accennare mai al formato della password.
- Non rivelare o suggerire la propria password in un modulo in internet.
- Non utilizzare mai l'opzione "ricorda password"
- Non utilizzare mai la password personale dell'organizzazione o di rete per un account internet, che non dispone di un accesso protetto (dove l'indirizzo browser web inizia con https:// invece di http:/).
- Segnalare eventuali sospetti concernenti la sicurezza della password ai tecnici informatici.

Ogni utente della rete Intranet dell'Istituto dispone di credenziali personali per accedere ai dispositivi presenti nei laboratori e nelle postazioni fisse

presenti nelle sedi.
Ad ogni utente viene creato dall'amministratore un account nominativo di dominio col quale può operare attraverso i dispositivi dell'Istituto nelle proprie aree di pertinenza (rete didattica o rete amministrativa), ha diritto ad operare solo ed esclusivamente nella propria area, non può installare software in nessun PC fisso.
Le attività nei diversi dispositivi che l'utente utilizza, i servizi Intranet e di stampa e l'accesso alla rete Internet viene quindi monitorata grazie al login effettuato sui dispositivi fissi.
Le credenziali di accesso vengono fornite dall'amministratore del sistema informativo nel momento della presa di servizio, per quanto riguarda il personale, o nell'ambito delle attività di accoglienza nella classe prima, per quanto riguarda gli studenti.

L'accesso alla rete WiFi è concesso solo al personale. La password di accesso alla rete viene fornita dall'amministratore del sistema informativo nel momento della presa di servizio. A seguito dell'accesso alla rete, per poter effettuare la navigazione occorre autenticarsi presso il gestore della rete (Federa - Lepida S.p.A.), che provvede anche al tracciamento del traffico Internet.

Ogni utente della rete Intranet e Internet è tenuto a:
- conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione;
- scollegarsi dal sistema (disconnettersi, effettuare il log-off) ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima;
- non lasciare un elaboratore incustodito connesso alla rete, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
- effettuare la sostituzione della/e password nel caso si sospetti una perdita di segretezza della stessa.

I referenti delle differenti aree (sistema informativo, sito, registro, Google Workspace, sistema di prenotazione aule, sistema fotocopiatori, blog) in qualità di super-admin, in busta chiusa, le proprie credenziali di accesso al pannello di controllo nella cassaforte presso l'Ufficio di Dirigenza.

Art. 9 - Tutela della privacy: garanzie generali

Tutte le operazioni relative all'uso della rete sono improntate alla tutela della privacy. Relativamente alla "tutela della persona ed altri soggetti rispetto al trattamento dei dati personali" si fa riferimento ai Documenti

disponibili sul sito ed agli Atti, predisposti dal Dirigente Scolastico, titolare del trattamento dei dati personali, in collaborazione con il Responsabile per la Protezione dei Dati personali.

Art. 10 - Disposizioni di legge e sanzioni

Al di là delle regole di buona educazione ci sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie. Alcuni esempi:

Reati informatici
La legge 547/93 individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:

- danneggiamento informatico;
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- frode informatica.

Reati non informatici
Sono da considerare reati non informatici tutti quei reati o violazioni del codice civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto:

- ingiuria;
- diffamazione;
- minacce e molestie.

Atti di vandalismo, di sabotaggio o furti, verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati.
A fronte di violazioni delle regole stabilite dalla politica scolastica, la scuola, su valutazione del Dirigente Scolastico, si assume il diritto di impedire l'accesso dell'utente ai servizi informatici dell'Istituto per un certo periodo di tempo, rapportato alla gravità.
La violazione o il dolo accertati, oltre all'intervento disciplinare del Consiglio di Classe, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'autorità giudiziaria.
Nel caso di infrazione consapevole da parte dei docenti o del personale non docente si interverrà per via amministrativa secondo le norme vigenti.

Diritto d'autore

II Diritto di autore è regolato dalla legislazione vigente sui Diritti d'Autore: Legge del 22 aprile 1941 n° 633, modificata dalla legge 3 maggio 2019 n.37 , che all'art.70 stabilisce : "Il riassunto, la citazione o la riproduzione di brani o di parti di opera e la loro comunicazione al pubblico sono liberi se effettuati per uso di critica o di discussione, nei limiti giustificati da tali fini e purché non costituiscano concorrenza all'utilizzazione economica dell'opera; se effettuati a fini di insegnamento o di ricerca scientifica l'utilizzo deve inoltre avvenire per finalità illustrative e per fini non commerciali".

In base alle vigenti norme sul diritto d'autore è vietato utilizzare le risorse dell'Istituto per:

- copiare/fotocopiare qualunque tipo di materiale, protetto da copyright;
- scaricare o duplicare materiale digitali, protetti da copyright.

Art. 11 - Norme conclusive

Il presente "Regolamento per la sicurezza informatica - Linee guida per l'uso delle risorse tecnologiche e di rete" è allegato al "Regolamento di Istituto" e pubblicato all'albo on line della scuola.
Il Dirigente scolastico ha il diritto di revocare l'accessibilità temporanea o permanente ai laboratori e/o all'utilizzo di strumenti tecnologici e/o alle piattaforme di Istituto a chi non si attiene alle regole stabilite.
Il personale scolastico, gli studenti e i genitori vengono informati della pubblicazione del presente documento.

Si allegano

- Regolamento di gestione utilizzo dei Laboratori Didattici e delle Attrezzature Tecnologiche
- Regolamento di gestione e utilizzo di Google Workspace
- Regolamento di gestione del Sito Web istituzionale
- Regolamento di gestione e utilizzo del Registro Elettronico
- Netiquette - etica e norme di buon uso dei servizi di rete
- Regolamento BYOD